

We claim:

1 1. Apparatus for monitoring a local area network (LAN)
2 through a remote administrative web site, the apparatus
3 comprising:

4 a service enablement platform (SEP) for connection
5 to the LAN and for connection, through a wide area
6 network (WAN) connection, to the administrative web site,
7 wherein the SEP comprises:

8 a processor;

9 a memory, connected to the processor, for
10 storing computer executable instructions therein; and

11 first and second network interfaces, operable
12 in conjunction with the processor, for communicatively
13 interfacing the SEP, through a first network connection,
14 to the WAN and, through a second network connection, to
15 the LAN, respectively;

16 wherein the processor, in response to execution
17 of the instructions:

18 continually monitors operational status of
19 a monitored entity so as to detect an alarm condition
20 resulting from an operational failure in the monitored
21 entity, the monitored entity comprising the SEP, at least
22 one of the first and second connections or at least one
23 of a plurality of servers residing on the LAN;

24 generates, in response to the alarm
25 condition, an alarm message containing information
26 related to the alarm condition;

27 converts the alarm message into a
28 predefined format suitable for communication over a web
29 connection so as to yield a web-communicable alarm
30 message; and

31 transmits the web-communicable alarm
32 message, via the WAN interface and the first network
33 connection, to the administrative web site which, in
34 response to receipt of the web-communicable alarm
35 message:

36 extracts the alarm information from
37 the web-communicable alarm message so as to define
38 extracted alarm information; and

39 updates a record in a database,
40 maintained by the administrative web site and associated
41 with the SEP, to reflect the extracted alarm information.

1 2. The apparatus in claim 1 wherein the processor, in
2 response to execution of the stored instructions:

3 forms an HTTP message containing the alarm
4 information; and

5 encrypts the HTTP message to form the
6 web-communicable message.

1 3. The apparatus in claim 2 wherein the SEP further
2 comprises a web client executed by the processor and the
3 administrative web site comprises a web server with the
4 HTTP message being transported, via the WAN and over a
5 web connection, from the web client to the web server.

1 4. The apparatus in claim 2 wherein the processor, in
2 response to execution of the stored instructions, signs
3 the HTTP message using a private key associated with the
4 SEP prior to encrypting the HTTP message.

1 5. The apparatus in claim 4 wherein the processor, in
2 response to execution of the stored instructions:
3 converts the alarm information in the alarm message
4 into extensible markup language (XML); and
5 forms the HTTP message as containing the XML.

1 6. The apparatus in claim 5 wherein the processor, in
2 response to execution of the stored instructions:
3 converts the alarm information message in the alarm
4 message into a corresponding WDDX hash structure; and
5 translates the WDDX hash structure into the XML.

1 7. The apparatus in claim 6 wherein the XML, into which
2 the WDDX hash structure is converted, is serialized.

1 8. The apparatus in claim 4 wherein the administrative
2 web site in response to receiving the HTTP message:
3 decrypts the HTTP message so as to define a
4 decrypted HTTP message;
5 authenticates the decrypted HTTP message using a
6 signature contained within HTTP message; and
7 if the decrypted HTTP message is authentic, updates
8 the record in the database in response to the alarm
9 information carried in decrypted HTTP message.

1 9. The apparatus in claim 8 wherein the administrative
2 web site:

3 converts XML contained within the decrypted HTTP
4 message into a received WDDX hash structure; and
5 updates the record in the database in response to
6 alarm information contained in the received WDDX hash
7 structure.

1 10. The apparatus in claim 1 further comprising the
2 administrative web site wherein the database contains a
3 plurality of customer records, where each of the
4 plurality of customer records is associated with a
5 corresponding one of a plurality of different SEPs and
6 each of the different SEPs is associated with a different
7 one of a plurality of LANs such that all of said LANs are
8 monitored through the administrative web site.

1 11. The apparatus in claim 1 wherein the WAN comprises
2 either a private or a publicly-accessible communications
3 network.

1 12. The apparatus in claim 11 wherein the publicly
2 accessible communications network is the Internet.

1 13. The apparatus in claim 1 wherein the processor, in
2 response to the stored instructions and if a plurality of
3 alarm messages exists, prioritizes and queues each of the
4 plurality of alarm messages from the SEP for transmission
5 to the administrative web site.

1 14. The apparatus in claim 1 wherein the administrative
2 web site downloads to the memory in the SEP a
3 corresponding pre-defined configuration profile which
4 specifies an operational and network environment of the
5 LAN for subsequent use in initializing the SEP.

1 15. The apparatus in claim 14 wherein the profile is
2 communicated through an HTTP message between the
3 administrative web site and the SEP.

1 16. The apparatus in claim 15 wherein the SEP further
2 comprises a web client executed by the processor and the
3 administrative web site comprises a web server with the
4 HTTP message being transported, via the WAN and over a
5 web connection, from the web client to the web server.

1 17. The apparatus in claim 15 wherein the administrative
2 web site signs the HTTP message using a private key
3 associated with the administrative web site prior to
4 encrypting the HTTP message.

1 18. The apparatus in claim 17 wherein the administrative
2 web site:
3 converts the profile into extensible markup language
4 (XML); and
5 forms the HTTP message as containing the XML.

1 19. The apparatus in claim 18 wherein the administrative
2 web site:

3 converts the profile into a corresponding WDDX hash
4 structure; and
5 translates the WDDX hash structure into the XML.

1 20. The apparatus in claim 19 wherein the XML, into
2 which the WDDX hash structure is converted, is
3 serialized.

1 21. The apparatus in claim 17 wherein the processor, in
2 response to receiving the HTTP message from the
3 administrative web site, and in response to the stored
4 instructions:

5 decrypts the HTTP message so as to define a
6 decrypted HTTP message;

7 authenticates the decrypted HTTP message using a
8 signature contained within HTTP message; and

9 if the decrypted HTTP message is authentic, stores
10 the profile contained in the decrypted HTTP message in a
11 database associated with the SEP.

1 22. The apparatus in claim 21 wherein the processor, in
2 response to the stored instructions:

3 converts XML contained within the decrypted HTTP
4 message into a received WDDX hash structure; and

5 updates the database in the SEP using the profile
6 contained in the received WDDX hash structure.

1 23. The apparatus in claim 14 further comprising the
2 administrative web site wherein the database contains a

3 plurality of customer records, where each of the
4 plurality of customer records being associated with a
5 corresponding one of a plurality of different SEPs, and
6 each of the different SEPs being associated with a
7 different one of a plurality of LANs such that all of
8 said LANs are monitored through the administrative web
9 site, and said each of the customer records having a
10 separate configuration profile associated with said one
11 of said LANs.

1 24. A method for use in apparatus for monitoring a local
2 area network (LAN) through a remote administrative web
3 site, the apparatus having: a service enablement platform
4 (SEP) for connection to the LAN and for connection,
5 through a wide area network (WAN) connection, to the
6 administrative web site, wherein the SEP comprises: a
7 processor; a memory, connected to the processor, for
8 storing computer executable instructions therein; and
9 first and second network interfaces, operable in
10 conjunction with the processor, for communicatively
11 interfacing the SEP, through a first network connection,
12 to the WAN and, through a second network connection, to
13 the LAN, respectively; the method comprising the steps,
14 performed by the processor and in response to execution
15 of the stored instructions, of:

16 continually monitoring operational status of a
17 monitored entity so as to detect an alarm condition
18 resulting from an operational failure in the monitored
19 entity, the monitored entity comprising the SEP, at least

one of the first and second connections or at least one of a plurality of servers residing on the LAN;

generating, in response to the alarm condition, an alarm message containing information related to the alarm condition;

converting the alarm message into a predefined format suitable for communication over a web connection so as to yield a web-communicable alarm message; and

transmitting the web-communicable alarm message, via the WAN interface and the first network connection, to the administrative web site which, in response to receipt of the web-communicable alarm message:

extracts the alarm information from the web-communicable alarm message so as to define extracted alarm information; and

updates a record in a database, maintained by the administrative web site and associated with the SEP, to reflect the extracted alarm information.

25. The method of claim 24 further comprising the steps, performed by the processor, of:

forming an HTTP message containing the alarm information; and

encrypting the HTTP message to form the web-communicable message.

26. The method of claim 25 wherein the SEP further comprises a web client executed by the processor and the administrative web site comprises a web server, and the

method further comprises the step of transporting the HTTP message, via the WAN and over a web connection, from the web client to the web server.

27. The method of claim 25 further comprising the step, performed by the processor, of signing the HTTP message using a private key associated with the SEP prior to encrypting the HTTP message.

28. The method of claim 27 further comprising the steps, performed by the processor, of:

converting the alarm information in the alarm message into extensible markup language (XML); and forming the HTTP message as containing the XML.

29. The method of claim 28 further comprising the steps, performed by the processor, of:

converting the alarm information message in the alarm message into a corresponding WDDX hash structure; and

translating the WDDX hash structure into the XML.

30. The method of claim 29 wherein the XML, into which the WDDX hash structure is converted, is serialized.

31. The method of claim 27 further comprising the steps, performed by administrative web site in response to receiving the HTTP message, of:

4 decrypting the HTTP message so as to define a
5 decrypted HTTP message;
6 authenticating the decrypted HTTP message using a
7 signature contained within HTTP message; and
8 if the decrypted HTTP message is authentic, updates
9 the record in the database in response to the alarm
10 information carried in decrypted HTTP message.

1 32. The method of claim 31 further comprising the steps,
2 performed by the administrative web site, of:

3 converting XML contained within the decrypted HTTP
4 message into a received WDDX hash structure; and
5 updating the record in the database in response to
6 alarm information contained in the received WDDX hash
7 structure.

1 33. The method of claim 24 wherein the database contains
2 a plurality of customer records, where each of the
3 plurality of customer records is associated with a
4 corresponding one of a plurality of different SEPs and
5 each of the different SEPs is associated with a different
6 one of a plurality of LANs such that all of said LANs are
7 monitored through the administrative web site.

1 34. The method in claim 24 wherein the WAN comprises
2 either a private or a publicly-accessible communications
3 network.

1 35. The method in claim 34 wherein the publicly
2 accessible communications network is the Internet.

1 36. The method in claim 34 further comprising the step,
2 performed by the processor, of if a plurality of alarm
3 messages exists, prioritizing and queuing each of the
4 plurality of alarm messages from the SEP for transmission
5 to the administrative web site.

1 37. The method of claim 24 further comprising the step,
2 performed by the administrative web site, of downloading
3 to the memory in the SEP a corresponding pre-defined
4 configuration profile which specifies an operational and
5 network environment of the LAN for subsequent use in
6 initializing the SEP.

1 38. The method of claim 37 further comprising the step
2 of communicating the profile through an HTTP message
3 between the administrative web site and the SEP.

1 39. The method of claim 38 wherein the SEP further
2 comprises a web client executed by the processor and the
3 administrative web site comprises a web server, and the
4 method comprises the step of transporting the HTTP
5 message, via the WAN and over a web connection, from the
6 web client to the web server.

1 40. The method of claim 38 further comprising the step,
2 performed by the administrative web site, of signing the

3 HTTP message using a private key associated with the web
4 site prior to encrypting the HTTP message.

1 41. The method of claim 40 further comprising the steps,
2 performed by the administrative web site, of:

3 converting the profile into extensible markup
4 language (XML); and
5 forming the HTTP message as containing the XML.

1 42. The method of claim 41 further comprising the steps,
2 performed by the administrative web site, of:

3 converting the profile into a corresponding WDDX
4 hash structure; and
5 translating the WDDX hash structure into the XML.

1 43. The method in claim 42 wherein the XML, into which
2 the WDDX hash structure is converted, is serialized.

1 44. The method in claim 40 further comprising the step,
2 performed by the processor in response to receiving the
3 HTTP message from the administrative web site and in
4 response to the stored instructions, of:

5 decrypting the HTTP message so as to define a
6 decrypted HTTP message;

7 authenticating the decrypted HTTP message using a
8 signature contained within HTTP message; and

9 if the decrypted HTTP message is authentic, storing
10 the profile contained in the decrypted HTTP message in a
11 database associated with the SEP.

1 45. The method of claim 44 further comprising the steps,
2 performed by the processor, of:

3 converting XML contained within the decrypted HTTP
4 message into a received WDDX hash structure; and

5 updating the database in the SEP using the profile
6 contained in the received WDDX hash structure.

1 46. The method of claim 37 wherein the database in the
2 administrative web site contains a plurality of customer
3 records, where each of the plurality of customer records
4 being associated with a corresponding one of a plurality
5 of different SEPs, and each of the different SEPs being
6 associated with a different one of a plurality of LANs
7 such that all of said LANs are monitored through the
8 administrative web site, and said each of the customer
9 records having a separate configuration profile
10 associated with said one of said LANs.